



FIGURE 8.9 A broadband connection requires a cable modem connected to a cable TV service line, a DSL modem connected to a phone line, or a satellite modem connected to a satellite dish. These aren't really modems but are so named because they are functionally similar to modems.

described in the next section, students can connect to the Internet while they move around a wireless-equipped campus, travelers can make Web connections while waiting in airports, and coffee shops can become Internet cafes for people with wireless receivers in their laptops.

Each of these broadband technologies is widely deployed in the United States, and each is expanding its area of coverage. The U.S. lags far behind many other countries, though, in terms of the speed, quality, and price of its broadband offerings. In Japan, for example, a person can download an entire movie in two minutes—a movie that would take two hours or more to download with a U.S. broadband connection that costs just as much as the Japanese service. There's considerable debate about why the country that created the Internet provides inferior Internet access for its citizens. At least part of the reason may be the U.S. government's reluctance to regulate the telecommunications industry the way other developed countries do. In any case, it's likely that broadband service in the U.S. and elsewhere will continue to broaden.

Wireless Network Technology

Wireless technology is a **liberating force**. It will make possible **human-centered computers**. This wasn't possible before because we were **anchored to a PC**, and we had to go to it like going to a temple to **pay our respects**.

—Michael Dertouzos, Director, MIT Laboratory for Computer Science

A lightning-fast network connection to your desktop is of little use if you're away from your desk most of the time. When bandwidth is less important than mobility and portability, wireless technology can provide practical solutions.

Infrared wireless technology has been around for many years. Many laptops and

handheld computers have infrared ports that can send and receive digital information over short distances, provided there are no physical barriers blocking the signals. Remote control devices use infrared beams to send commands to TVs, sound systems, and other home entertainment devices. Infrared technology isn't widely used in networks because of distance and line-of-sight limitations.

The fastest-growing wireless LAN technology is known as **Wi-Fi**. Wi-Fi uses radio waves to link computers to a LAN through a nearby **wireless access point (WAP)**—a Wi-Fi **hotspot**. (Apple calls their wireless access points *AirPort hubs*; some companies label theirs as *Wi-Fi routers*.) A wireless access point is similar to a network hub; it serves as a central connection point for wireless computers, PDAs, phones, media players, digital cameras, game consoles, security devices, and more. (Wi-Fi technology also allows peer- to-peer communication, so that two Wi-Fi—equipped devices can communicate directly with each other. But most Wi-Fi communication goes through wireless hubs.) If the access point is wired into a LAN, wireless devices can communicate with wired devices on the LAN. If the access point is linked to a DSL modem, cable modem, or a direct Internet connection, the access point is an Internet hotspot—a wireless gateway to the Internet.

Wi-Fi doesn't have the bandwidth of a hard-wired Ethernet connection, but it's fast enough for most applications, including multimedia Web downloads. There are several different flavors of Wi-Fi; all are variations of the IEEE 802.11 specifications for wireless local area networks. In the early 2000s, most Wi-Fi devices followed the 802.11b standards. Because of their greater bandwidth and range, 802.11g devices quickly took over the Wi-Fi market. Today 802.11n, with up to three times the bandwidth of 802.11g, is emerging as the new standard. Devices from different Wi-Fi generations can coexist on the same wireless networks, but older 802.11b devices can slow traffic down for everybody on a network.

Wi-Fi devices use the 2.4GHz and 5GHz band of the radio spectrum. Many common devices, including portable phones and microwave ovens, can cause Wi-Fi interference, especially on the crowded 2.4GHz band. Wi-Fi devices can transmit on different *channels* within each band, so it's often possible to reduce interference by changing channel settings on Wi-Fi hub devices. Wi-Fi range is affected by a number of factors—nearby objects that block signals, antenna placement, and devices competing for the same part of the radio spectrum (including other Wi-Fi networks in the neighborhood). A typical Wi-Fi access point has a range of up to 120 feet indoors and 300 feet outdoors. Installing additional access points can extend the range of a network.

Millions of homes, schools, campuses, and businesses worldwide have Wi-Fi networks. Hundreds of thousands of public hotspots have been installed in coffee houses, airports, restaurants, libraries, and other public buildings. A home Wi-Fi network allows computers to connect from any room without cables. Wi-Fi hotspots are common in airports, coffee shops, hotels, and other public places. A growing number of cities and towns are building citywide Wi-Fi networks, although some metropolitan Wi-Fi networks have been delayed or blocked for technological and political reasons.

Many public hotspots and Wi-Fi networks are free and open to all devices within range. Others require visitors to agree to terms of service before connecting to the Internet. Still others require passwords and other forms of authentication. Some charge for access by the month or by the hour. But free Wi-Fi access points are sprouting everywhere, part of a grassroots movement to provide universal wireless access to the Net.

There's a growing interest in another radio-based wireless standard called **WiMAX** or **802.16**. A single WiMAX tower can provide Wi-Fi-style access to a 25-square-mile area—the same area that can be covered by a cell phone tower. WiMAX also supports line-of-sight connections to customers up to 30 miles away. WiMAX isn't designed to replace Wi-Fi, but it can be a powerful tool for connecting Wi-Fi networks.

Wireless networks raise many security concerns. A wireless access point broadcasts information in all directions; the network forms a sphere with a diameter of up to 300 feet (the length of a football field). If the network is not secured, a technically skilled snooper



FIGURE 8.10 A wireless Internet connection is created by linking a wireless access point like one of these to a broadband or direct Internet connection.

with a laptop inside this virtual sphere can “sniff” network traffic and read what you’re writing and collect email addresses and other personal information. The **WEP** (wired equivalent privacy) encryption scheme (see Chapter 10) improves the security of wireless networks by making your data as secure as it would be on a wired Ethernet. Businesses that need extra security for their wireless networks can take two additional steps: They can treat their wireless network as an insecure network and put a **firewall** between their wireless network and their wired network. (A firewall blocks unauthorized data transfers. We’ll discuss how firewalls work in Chapter 10.) They can also make a wireless network more secure through the use of a **VPN (virtual private network)**. A VPN is an electronic “tunnel” through the Internet that uses encryption and other security measures to keep out unauthorized users and prevent eavesdropping.

Another type of wireless technology is **Bluetooth**, or **802.15**, named for a Danish king who overcame his country’s religious differences. Bluetooth technology overcomes differences between mobile phones, handheld computers, and PCs, making it possible for all of these devices to communicate with each other regardless of their operating systems. Bluetooth uses radio technology similar to that of Wi-Fi, but its transmissions are limited to about 30 feet. Bluetooth isn’t designed to compete with Wi-Fi. It is intended to replace the wires that connect devices such as cell phones, headsets, PDAs, and printers to each other. With Bluetooth it’s possible to create a **personal area network (PAN)**—a network that links a variety of personal electronic devices so they can communicate with each other.

Bluetooth applications include:

- Linking a mobile phone to a wireless headset or a car’s audio system
- Connecting a wireless keyboard and mouse to a computer
- Connecting a wireless game controller to the game console
- Sharing contact information and calendars between PDAs and/or mobile phones

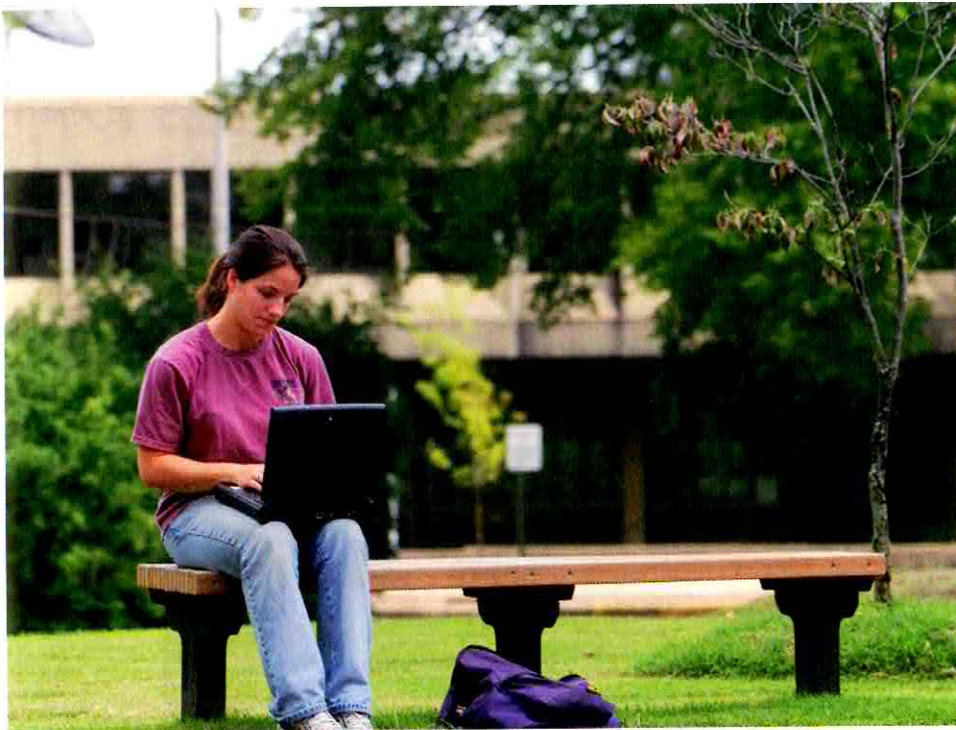


FIGURE 8.11 This University of Tennessee student can connect to the Internet using the campus wireless network.

Bluetooth technology is currently limited to simple device connectivity, but in the future it will open up all kinds of possibilities:

- A pacemaker senses a heart attack and notifies the victim's mobile phone to dial 911.
- A car radio communicates with parking-lot video cameras to find out where spaces are available.
- A medical wristband transmits an accident victim's vital information to a doctor's hand-held computer.
- A cell phone tells you about specials on clothes (available in your size) as you walk past stores in a mall. (Many fear that this technology will usher in a new era of junk phone calls.)

Wi-Fi and Bluetooth networks aren't nearly as widely used as wireless mobile phone networks. In two decades, mobile phones have gone from simple analog systems to powerful digital devices that can handle Internet data, text messages, photos, and other data along with voice traffic.

Mobile phone Internet connections are more common in Europe and Asia than they are in the United States, but the USA is catching up. While many Americans enjoy sending text messages and sharing photos with their cell phones, phone users in Europe and Asia are more likely to use their phones as multifunction devices. In Japan, for example, people routinely use their phones to send and receive email, check news headlines, shop, play games, share photos and short video clips, and even do karaoke.

The emerging generation of mobile wireless technology, often called **3G**, uses high-bandwidth connections to support true multimedia. Many mobile phone companies are using 3G technology to make phones into all-purpose digital devices.

There's a tremendous overlap in the capabilities and potential of Wi-Fi, WiMAX, and 3G. How we use these technologies will depend in part on how telecommunications companies develop them. In any case, the boundaries that separate phone networks and computer networks will continue to blur.



FIGURE 8.15 A server might look like a normal PC. But industrial-strength servers such as these powerful IBM devices can provide software and data for hundreds or thousands of networked computers.

between machines. But unlike a PC operating system, the NOS must respond to requests from many computers and must coordinate communication throughout the network. Today many organizations are replacing the specialized PC-based NOS with an **intranet** system—a system built around the open standards and protocols of the Internet, as described in more detail in the next chapter.

The function and location of the network operating system depend in part on the LAN model. Some LANs are set up according to the **client/server model**, a hierarchical model in which one or more computers act as dedicated servers and all the remaining computers act as **clients**. Each server is a high-speed, high-capacity computer containing data and other resources to be shared with client computers. Using NOS server software, the server fulfills requests from clients for data and other resources. In a client/server network, the bulk of the NOS resides on the server, but each client has NOS client software for sending requests to servers. Many small networks are designed using the **peer-to-peer model** (sometimes called **p-to-p** or **P2P**), which enables every computer on the network to be both client and server. In this kind of network, every user can make files publicly available to other users on the network. Some desktop operating systems, including many versions of Windows and the Mac OS, include all the software necessary to operate a peer-to-peer network. In practice, many networks are hybrids that combine features of the client/server and peer-to-peer models.

Outside of a LAN, the most basic type of communication software is primitive **terminal emulation software**, which enables a computer to function as a character-based “dumb” terminal—a simple input/output device for sending messages to and receiving messages from the host computer. A terminal program handles phone dialing, protocol management, and the miscellaneous details necessary for making a PC and a modem work together. With terminal software and a modem, a PC can communicate through phone lines with another PC, a network of computers, or, more commonly, a large multiuser computer. The Windows, Mac, and Linux operating systems include terminal emulation programs.

At the other end of the line, communications software is usually built into the multiuser operating system of the **host system**—the computer that provides service to multiple users. This software enables a timesharing computer (see Chapter 1) to communicate with several other computers or terminals at once. The most widely used host operating system today is UNIX, the 40-year-old OS that has many variants, including the open source Linux OS discussed in Chapter 4.

Basic terminal emulators are fine for bare-bones computer-to-computer connections, but their character-based user interfaces can be confusing to people who are used to point-and-click graphical user interfaces. What’s more, they can’t be used to explore media-rich destinations on and off the Web. That’s why most online explorers today use Web browsers and other graphical client software instead of generic terminal programs.

The Network Advantage

A network becomes more valuable as **it reaches more users**.

—Metcalfe’s Law, by Bob Metcalfe, inventor of Ethernet

With this background in mind, let’s reconsider the three reasons people use networks:

- *Networks enable people to share computer hardware resources, reducing costs and making it possible for more people to take better advantage of powerful computer equipment.* When computers and peripherals are connected in a LAN, computer users

can share peripherals. Before LANs, the typical office had a printer connected to each computer. Today it's more common to find a large group of computers and users sharing a small number of high-quality networked printers. In a client/server network, each printer may be connected to a *print server*—a server that accepts, prioritizes, and processes print jobs. Although it may not make much sense for users to try to share a printer on a wide area network (because it's not particularly convenient to use a printer that's hundreds of miles away), WAN users often share other hardware resources. Many WANs include powerful mainframes and supercomputers that can be accessed by authorized users at remote sites. Later in this chapter, we'll discuss grid computing—using grids of networked computers to share processing power and storage.

- *Networks enable people to share data and software programs, increasing efficiency and productivity.* In offices without networks, people often transmit data and software by “sneakernet”—that is, by carrying discs and flash drives between computers. In a LAN, one or more computers can be used as *file servers*—storehouses for software and data that are shared by several users. With client software, a user can, without taking a step, *download* software and data—copy it from a server. Of course, somebody needs to *upload* the software—copy it to the server—first. A large file server is typically a dedicated computer that does nothing but serve files. But a peer-to-peer approach, allowing any computer to be both client and server, can be an efficient, inexpensive way to share files on small networks. (There's more on file sharing later in the chapter.) Of course, sharing computer software on a network can violate software licenses (see Chapter 4) if not done with care. Many, but not all, licenses allow the software to be installed on a file server as long as the number of simultaneous users never exceeds the number of licensed copies. Some companies offer *site licenses* or *network licenses*, which reduce costs for multiple copies or remove restrictions on software copying and use at a network site. Networks don't eliminate compatibility differences between different computer operating systems. Users of Windows-compatible computers, for example, can't run Mac applications just because they're available on a file server. But they can, in many cases, use data files and documents created on a Mac and stored on the server. For example, a poster created with Adobe Illustrator on a Mac could be stored on a file server so it can be opened, edited, and printed by Illustrator users on Windows PCs. File sharing, however, isn't always that easy. If users of different systems use programs with incompatible file formats, they need to use *data translation software* to read and modify each other's files. On WANs (or the Internet), the transfer of data and software can save more than shoe leather; it can save time. There's no need to send printed documents or discs by mail between two sites if both sites are connected to the same network.

- *Networks enable people to work together, play together, and communicate in ways that are difficult or impossible without network technology.* Some software applications can be classified as *groupware*—programs designed to enable several networked users to work on the same documents at the same time. Groupware programs include multiuser appointment calendars, project-management software, database-management systems, and software for group editing of documents. Many groupware programs today, such as IBM Lotus Notes, are built on standard Internet protocols, so group members can communicate and share information using Web browsers and other standard Internet software tools. Groupware programs are commonly used in large businesses and institutions where information technology specialists manage hundreds or thousands of computers. But most groupware functions—email, message posting, calendars, and the rest—are available to anyone through other Web and PC applications. In fact, networks offer all kinds of communication possibilities to people inside and outside the business world.

In the next section, we'll focus on the third point—the communication and collaboration possibilities of networks. Then we'll revisit the first two points—the sharing of hardware and software—and see how they're tied in with interpersonal communication, too.

How It Works

8.1 A Home Computer Network

1. A cable or DSL line provides high-bandwidth access to the Internet.



2. A cable modem or DSL modem connects your home network to an Internet service provider. It converts the analog signal entering your house into a digital signal and vice versa.

3. A combination router/firewall/hub manages traffic on your home network. The hub lets you connect multiple networked devices. The router takes data packets coming in over one network link and sends them out over a link leading to the packet's destination. The firewall prevents unauthorized packets from being forwarded over the network.

4. A PC contains a network card rated at 100 Mbps —100 million bits per second. (Older, slower cards support only 10 Mbps).

5. Cat 5e cables connect Ethernet-equipped devices. The cables look like telephone cables, but the connectors are slightly different. Cat 5e cables are easier to work with than older coaxial cables.

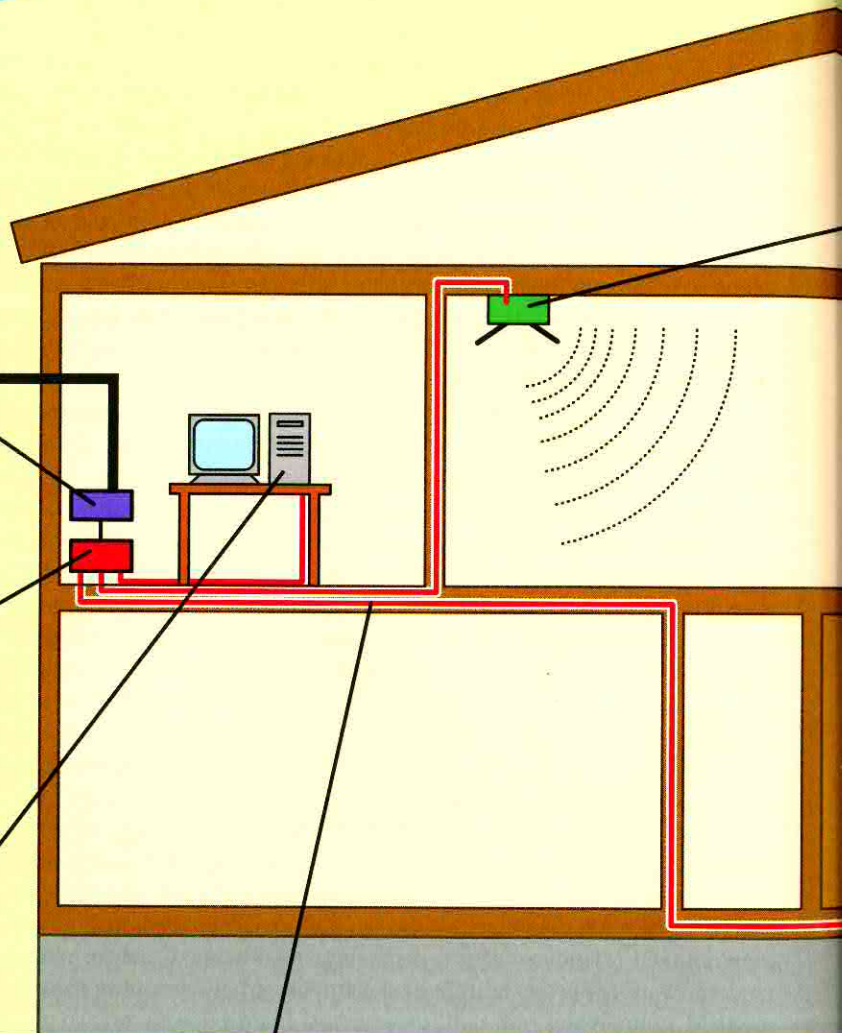


FIGURE 8.16

6. A wireless access point connects Wi-Fi devices with the rest of the network. To maximize reception, the Wi-Fi device is placed in a central location not obstructed by large metal objects.

7. A PC with a Wi-Fi card communicates with the rest of the network without a wired connection. Its connection will be slower than the connection of the Ethernet-equipped PC.

8. A networked printer can be shared by all of the devices on the home network. Some printers contain network cards with Ethernet ports, allowing them to connect to the network just like PCs. Other printers contain only USB ports designed for connecting them to individual host PCs. The USB printer shown here is shared by its host PC with other computers on the network.

9. A notebook computer with built-in Wi-Fi can access the network from anywhere in the house or the yard.

10. A video game console connected to the network with Ethernet lets you play multi-player games.

11. The WEP key and 128-bit encryption help keep outsiders off your wireless network.